

Electronic identification

BY CHESTER HICKS

Which states have legislation regarding digital signatures?

In an era of electronic commerce, communication and correspondence, states have recognized the importance of authentication of electronic documents through the use of digital signatures. As of November 1999, at least 29 states had legislation regulating the use of digital signatures.

A digital signature is but one type of electronic signature. Other types of electronic signatures include digitized renditions of inked signatures and biometric signatures using fingerprints or retinal scans, which may be scientifically traced to a particular person. Digital signatures are the most established types of electronic signature. Most state laws and methods on this technology address digital signatures.

A digital signature is a number that is transmitted with an electronic message to identify the message's sender or recipient. Because the number provides authentication to a document, it has the same function as a written signature. Thus, the number is called a "digital signature" — but it is not a digitized handwritten signature.

A digital signature is a pair of mathematical programs called a "key pair." Each "key" is merely a long sequence of 0s and 1s, or binary digits. A key may also be represented as an alphanumeric sequence that is much shorter than the binary sequence, yet still very long. A key pair consists of a "public key" and a "private key." The two keys are mathematically related, but one cannot be used to determine the other. Either key can, however, be used to scramble, or encrypt, a message. The other key in the pair is the only key that can be used to unscramble, or decrypt, the information.

For example, a computer user can create a key pair using widely available software. The key-pair owner can then freely share his or her public key with others. Anyone wishing to communicate with the key-pair owner uses the key pair owner's public key to encrypt a message and send it to the key pair owner. The recipient, the key-pair owner, uses his or her private key to decrypt the message. Because only one private key will decrypt a message encrypted with the matching public key, the sender is assured that only the intended recipient may read the message.

Therefore, a digital signature involves two steps — creation and verification. The signer creates the digital signature by applying the private key of the sender to the

contents of the message. The receiver then verifies the message by referring to the message and the public key.

The authentication of digital signatures intertwines technology and the law. Signatures have special significance in legal transactions. Certain formalities are generally required for legal transactions to be considered valid. These legal purposes are achieved if the signer and the document can be authenticated and the transaction is marked by an event. A signature should indicate who signed the transaction and should be difficult for anyone else to reproduce without authorization.

Legislation addressing the use of digital signatures varies. Utah's SB 188, reprinted in The Council of State Governments' 1997 volume of *Suggested State Legislation*, amended the Digital Signature Act of 1995. The law, which was the first to authorize the use of digital signatures, governed the use of

public and private key pairs and certification authorities.

Other states that have adopted legislation include California, Mississippi, New Mexico, Virginia and Washington. The laws of each vary greatly. For example, California law governs only digital signatures affixed to communications with public entities. The law provides that a digital signature has the same effect as a manual one if it is unique to the person using it, capable of verification, under the sole control of the person using it and linked to the substance so that any alteration invalidates the signature. On the other hand, some states have general legislation pertaining to electronic signatures, with digital signatures as merely one alternative.

The emerging technology of digital signatures can provide a computer-based alternative to traditional signatures for a wide variety of transactions. With a secure key pair, a message can be transformed to a code that remains private until it is received at its intended destination. With this key pair also comes verification of the contents of the message itself. A number of approaches have recently been enacted as states address the regulation of electronic authentication. In the 21st century, lawmakers will continue to be left with the challenge of deciding how best to deal with this technology that is sure to have a profound impact on the lives of their citizenry.

For more information on this or other topics, contact The Council of State Governments' States Information Center at (606) 244-8253 or e-mail sic@csg.org or visit CSG online at www.csg.org.



A digital signature authenticates an electronic document.

Chester Hicks is Southern regional coordinator with CSG's States Information Center.